ORIGINAL ARTICLE

Blockchain Adoption Drivers: The Rationality of Irrational Choices

Tommy Koens MSc[1] | Pol Van Aubel MSc[1] | Erik Poll PhD[1]

[1]Institute for Computing and Information Sciences,Radboud University, Nijmegen, 6525 EC Nijmegen, The Netherlands

Correspondence
Tommy Koens, Institute for Computing and Information Sciences,Radboud University, Nijmegen, 6525 EC Nijmegen, The Netherlands
Email: tkoens@cs.ru.nl

Funding information
Tommy Koens is supported by ING.
Pol Van Aubel is supported by the EU Regional Development Fund (EFRO), as part of the project BES (Betuwse Energie Samenwerking).

There has been a huge increase in interest in blockchain technology. However, little is known about the drivers behind the adoption of this technology. In this paper we identify and analyze these drivers, using six real-world and representative scenarios. We confirm in our analysis that blockchain is not an appropriate technology for some scenarios, from a purely technical point of view. The choice for blockchain technology in such scenarios may therefore seem as an irrational choice.

However, our analysis reveals that there are non-technical drivers at play that drive the adoption of blockchain, such as philosophical beliefs, network effects, and economic incentives. These non-technical drivers may explain the rationality behind the choice for blockchain adoption.

KEYWORDS
blockchain, distributed ledger, adoption, non-technical drivers

1 | INTRODUCTION

[1]Blockchain technology has received a huge interest ever since its inception in the cryptocurrency Bitcoin [**?**]. Indeed, on a global scale companies and governments [**?**] are looking for applications of this technology [**?**]. Cryptocurrencies, in particular Bitcoin, are the best-known and most successful scenario where blockchain technology has been adopted, but many other applications of blockchain have been proposed, such as supply chain management[**?**], identity management[**?**], and smart energy grids [**?**].

[1]This is an extended and revised version of a preliminary conference report that was presented in LSDVE2018[**?**]

However, the justification for using a blockchain in many of these scenarios is unclear. Indeed, many papers have argued that using a blockchain is not the best – or not even a good – solution for particular scenarios [**?**]. This has led to the proposal of methodologies for deciding if blockchain is an appropriate solution for a given scenario, from a technical point of view [**? ?**]. However, non-technical drivers are typically not discussed in most of the computer science literature. In this paper we try to look beyond this technical view, and we also consider the non-technical drivers behind the choice for blockchain in real-world scenarios.

To do this, in Section 3 we consider six real-world scenarios in which blockchain technology is used, namely, the cryptocurrency Bitcoin, the identity management solution uPort, a supply chain scenario for agricultural products, namely table grapes, the BikeBlockchain, a medical record use case, and a smart grid scenario. Here we also identify and analyze the drivers behind the adoption of blockchain for these scenarios. We distinguish five categories of drivers: technical properties, philosophical beliefs, network effects, economic incentives, and breaking the gridlock. Furthermore, we discuss the appropriateness of blockchain technology for each scenario. We argue that using a blockchain is not an appropriate solution for most of the scenarios if we only take a technological perspective. This may seem that using blockchain in these scenarios is an irrational choice. Based on this analysis, Section 4 discusses the non-technical drivers that may explain blockchain adoption. Here we argue that there is a rationality behind blockchain adoption if we also take non-technical drivers into account. Section 5 discusses related work, Section 6 future work, and Section 7 summarizes our conclusions.

2 | BACKGROUND

This section provides a generic description of blockchain technology and introduces the decision model by Wüst and Gervais [**?**] for determining if blockchain technology is appropriate for a particular scenario.

The novel part of blockchain technology is having a consortium of unknown participants to reach consensus [**?**]. Typically, participants in blockchain technology consist of users and miners. At any time, a user may propose a new state of the ownership of a token by means of a transaction. A transaction, contains at least the sender's account, the receiver's account, the number of tokens transferred, a timestamp and a signature of the sender.

Miners propose new ledger states, but only after having solved a cryptographic puzzle. The idea here is to prevent multiple, different ledger states being proposed. The participant who first solves the puzzle is allowed to propose a new state of the ledger. Miners propose new ledger states by collecting user transactions and proposing these as a set, called a block. Since the unique identifier of the previous block is included in the new proposed block, a chain of blocks is created, hence the term blockchain.

Blockchain may be useful in a scenario which contains certain properties. Therefore, to determine if blockchain is an appropriate technology for a particular scenario, several blockchain decision models have been proposed.

2.1 | Blockchain Decision Models

Wüst and Gervais [**?**] proposed a model to determine if blockchain technology is appropriate for a particular problem. Several such models have been proposed, as discussed by Koens and Pol [**?**]. We chose the model of Wüst and Gervais because it provides a detailed description of the decisions that have to be made, leaving less room for misinterpretation. Their model consist of a decision tree based on the following scenario properties:

(a) *Storing state.* Refers to the need of storing data that may change both in volume and in content over time.

(b) *Number of writers.* Multiple writers (also known as miners) must be present, that have a common interest in agreeing on the validity of the stored state.

(c) *Is there a Trusted Third Party?* A Trusted Third Party (TTP) is a centralized entity that could manage changes and updates the state. A TTP, if present, may also control who can read the state stored.

(d) *Are all writers known?* This refers to knowing the identity of all writers.

(e) *Are all writers trusted?* When writers are trusted, they are expected not to behave maliciously. When writers are not trusted, they may behave maliciously.

(f) *Public verifiability of state.* This property determines who may read the state stored on the blockchain, and verify the integrity of the ledger.

Based on these six properties, the model determines one of four possible solutions as the best solution for the scenario:

1. *Permissionless blockchain.* Anyone may join the network and read from the state stored, and write to the blockchain.

2. *Public permissioned blockchain.* A limited set of participants may write to the blockchain. Anyone may join the network and read the state.

3. *Private permissioned blockchain.* A limited set of participants may join the network, and write a new state. Only this set can read the state.

4. *Don't use blockchain.* This end state is reached when one of the properties (a), (b), (c), or (e) above is not met.

3 | SCENARIOS

The following sections present six scenarios in which blockchain is used. We chose these for two reasons. First, these are real-life and representative scenarios where a blockchain is used. Second, these scenarios are generally well known to be related with blockchain technology. For each scenario we propose a set of blockchain adoption drivers (see Table 1, page 18) and we group these drivers into:

- *Scenario properties.* These drivers, (a)-(f) above, focus on the rationale for using blockchain.
- *Philosophical beliefs.* These drivers focus on the rationale for using blockchain based on the participants' beliefs.
- *Network effects.* Here we propose drivers where existing participants influence new participants in using blockchain technology.
- *Economic incentives.* These drivers are based on financial gain, or preventing potential financial losses, by one of the parties involved in the scenario.
- *Breaking the gridlock.* Despite that blockchain may not be the best technical solution for some use cases, it may break down organisational barriers inducing organisations to work together. Furthermore, a third party managing this technology may also induce organisations to collaborate, as specific technological knowledge may not be present at some organisations.

The scenario properties are inherent characteristics of a scenario, which we consider *technical properties*. These properties often can be clearly and objectively measured, for example, the number of participants. The other four driver categories are about preferences or motivations for the use of blockchain as stated in the scenarios. We select these categories after an analysis of the scenarios and grouping of these preferences and motivations. These four cate-

gories of drivers are typically hard to measure as they are more subjective, and we consider these to be *non-technical properties*.

Categorization of these five categorized drivers is important because it allows us to determine what drives blockchain adoption. In Table 1 we summarize the analyses of the use cases discussed in Sections 3.1-3.6.

3.1 | Scenario 1 - Bitcoin

Scenario description.

In Nakamoto's work [**?**] a decentralized payment system is envisioned. The essence is to have a consortium of unknown participants achieve consensus [**?**]. To achieve this, Bitcoin uses a public permissionless blockchain, allowing anyone to participate.

Each participant owns one or more Bitcoin accounts. An account is identified by a public cryptographic key, and managed by the corresponding private key. Each account may hold a number of tokens, which represent a value, and can be seen as 'coins'. Coin ownership can be transferred by transactions. A transaction, in principle, contains the account of the sender, the account of the receiver, the number of coins transferred, and the signature of the sender. Transactions created by participants are collected by other participants called miners. These miners independently solve a moderately-hard cryptographic puzzle. The miner that solves the puzzle first, obtains the privilege to propose a new state of accounts, based on the transactions collected. A miner proposes a new state by presenting a sequence of transactions called a block. Note that only miners may write to the blockchain. Each block holds the hash of its previous block, linking all blocks into a block-chain.

Scenario properties.

This scenario has all the properties for the use of blockchain to be the right solution according to the scheme of Wüst and Gervais: we have to store state, there are multiple writers, there is (by design) no Trusted Third Party (TTP), the writers are unknown and untrusted, and the state should be publicly verifiable. In other words, the properties of this scenario provide a clear technical rationale to use blockchain.

Philosophical beliefs.

Bitcoin's pseudonymous inventor Nakamoto states that 'What is needed is an electronic payment system based on cryptographic proof instead of trust' [**?**]. Clearly, Bitcoin is specifically designed not to have a TTP. Also, many of its participants are motivated by political reasons to use Bitcoin [**?**]. For example, when national governments prevented WikiLeaks from receiving donations by blocking credit card transactions [**?**], Bitcoin could be used as an alternative payment system to circumvent these restrictions. Furthermore, given the pseudonymous nature of all accounts in Bitcoin, payments are more privacy-friendly than centralized bank payments.

Network effects.

Bitcoin has received considerable media attention in the last few years [**? ? ?**]. This causes a network effect, where people consider Bitcoin 'cool to use' [**?**]. Also, at this point in time several issues remain which hinder global adoption, such as scalability [**?**], high transaction fees, price volatility and energy consumption [**?**]. These problems are hard to solve, which has led to a growing academic interest in blockchain technology to tackle them [**? ?**].

Economic incentives.
Several companies have a direct economic interest in the success of Bitcoin. As miners nowadays need special dedicated hardware, hardware vendors supplying this hardware have a clear economic interest in the success of Bitcoin. Furthermore, many companies, including established firms and young startups [**?**], offer blockchain consultancy services, some of which are related to Bitcoin. These companies also have a strong economic incentive, namely to sell consulting services.

Finally, given the broad global attention to blockchain technology, there is the fear of missing out (FOMO) [**?**]. This may lead to that some parties buy bitcoins, as well as other cryptocurrencies, to mitigate the risk of having missed the bandwagon when it turns out the technology becomes a success. For example, public media has extensively reported on the rise of the value of Bitcoin. This triggered other, new participants also to invest in Bitcoin, as these participants also hope for a profitable investment in Bitcoin. Indeed, uninformed participants consider Bitcoin to be an alternative investment [**?**]. However, as Bitcoin is not backed by any government nor gold, these investments are fueled largely by speculation.

Breaking the gridlock.
In this scenario blockchain technology is a technical solution to the problem of reaching consensus amongst a consortium of unknown and unbound number of participants. There is no particular aim to break down organizational barriers, nor is there a third party that wants to trigger organisational collaboration.

3.2 | Scenario 2 - uPort

Scenario description.
This second scenario addresses an identity management solution. Such solutions aim to facilitate the management of identifiers, authentication, personal information, and the presentation of this information to other parties. Typically, in these solution schemes, a trusted identity provider such as a government, issues attributes to a participant. These participants store their attributes on their mobile device. This allows a verifying party such as a retailer, to verify the validity of the attributes issued.

Several companies (e.g. Consensys, Evernym, and IBM) advertise their block-chain-based identity solution. Here we focus on uPort [**?**] by Consensys. uPort is an identity management solution that uses the Ethereum blockchain [**?**] for so-called account recovery. In this account recovery process the user reclaims ownership of a unique number, called a persistent identifier (PI). This then allows participants to easily (re-)obtain attributes from issuing parties, by proving ownership of this PI.

The uPort app allows a device, such as a smart phone, to connect to a specific smart contract on Ethereum. This contract contains a unique number represented by the PI, which is linked to the participant's public key. When, for example, the device holding the attributes and private key is lost, a participant may prove to be the owner of the PI. Ownership of this PI is proven by requesting multiple trusted parties to state that, indeed, the participant is linked the unique number, after which the user can link a new public key to the PI. Currently, uPort seems to be the only identity management solution that offers recovery of a PI.

Scenario properties.
In this scenario, state in the form of a smart contract is stored on the publicly verifiable Ethereum blockchain. From a participant perspective, all writers to the contract holding the persistent identifier are known, since these are the parties (e.g. friends or government) trusted by the participant. In this scenario the owner of a smart contract, including

its trustees, can write to the contract. Furthermore, a centralized party, for example the issuing party of the attributes, could store the unique number related to the attributes of a participant. Therefore, following the model of Wüst and Gervais [**?**], there is no technical rationale to use blockchain technology in this scenario as all writers are trusted.

Philosophical beliefs.
The mission of uPort states that "we believe that everyone has the right to control their own digital identity" [**?**]. Blockchain technology offers a platform that can be used by everyone and, therefore, using a blockchain is in the interest of uPort. From a company perspective, offering such a platform is based on principles that drive uPort, such as company purpose, economic principles, and social impact. However, from a technical perspective there is no need to use blockchain for the unique number recovery, as explained above.

Network effects.
Blockchain technology offers multiple functionalities, such as storing of data, reaching consensus, and an audit trail. As companies often wonder how blockchain functionalities can benefit their company, curiosity may have played a role in blockchain adoption in this scenario.

Economic incentives.
The uPort app points to a perceived single source of truth, the blockchain. When more participants would adopt the uPort app, uPort would gain more exposure, recognition, and funding. Still, the need for blockchain technology can be questioned. Ethereum, despite its novel design, currently contains several issues such as scalability [**?**], energy consumption [**?**], and lack of decentralization[**?**]. Instead, an independent group of trusted third parties could be used to manage the unique identifier of the smart contract. However, blockchain technology is also a marketing tool to arouse interest in a product [**?**] which in this scenario is the identity solution, or to arouse interest in an organization [**?**] [**?**].

Breaking the gridlock.
Using a blockchain in this scenario triggered the collaboration between uPort, Ethereum, the municipality of Zug (Switzerland), and its inhabitants. By using blockchain an incentive is created to collaborate between these parties.

Additionally, uPort manages the necessary technology to register citizen's of Zug on the Ethereum blockchain, unlocking access to government eServices and proof of residency [**?**]. Here a third party managing the technology also triggers organisational collaboration.

3.3 | Scenario 3 - Agricultural Products Supply Chain

Scenario description.
In this third scenario a public permissioned blockchain called Hyperledger Fabric by IBM [**?**] is used. This blockchain tracks certificates in a supply chain of table grapes. In this scenario [**?**], a farmer in South Africa produces organic grapes, and presents such a claim to a certification authority. This authority issues a certificate to the farm, allowing the farm to certify its grapes. Grapes are stored in boxes, which are identified by a unique barcode.

To ensure a correct certification process, certification authorities are accredited by an accreditation authority. The certification authority stores the certificate it receives from an accreditation authority on the blockchain. Additionally, details of the certification authority are stored on the blockchain, so that anyone may see which party certified a farm. This entire process is audited. An auditor may revoke the certificate issued by the certification authority, for

example, after the discovery of unauthorized pesticides [**?**] being used in the production of the fruits. An auditor also may revoke accreditations made by the accreditation authority. Here, both revocation types are recorded on the blockchain.

The grape boxes are shipped to resellers in Europe, after which the grapes are sold to supermarkets, and eventually to customers. Since it is unknown who may purchase the grapes, public verifiability is required. This allows all parties involved to query the blockchain for the validity of the organic certificate. Also, change of ownership is recorded in the blockchain, and provenance of the labeled boxes can be determined. From this description we observe that there are multiple, known writers. However, these writers are not trusted, as can be observed from the cascading audit trail from farmer to auditor.

Scenario properties.

In this scenario the origin and background of the grapes are stored on the blockchain. Furthermore, multiple writers are present, such as certificate authorities and auditors. Finally, the state stored must be publicly verifiable, as consumers verifying the grape origins must read from the blockchain. Furthermore, in this scenario it is clear that writers are not trusted, because there exists an extensive audit trail. However, blockchain technology does not replace the audit trail. In this scenario blockchain technology introduces a decentralized administrative system in which audit findings are stored. In fact, even with blockchain technology, audits still must be performed to ensure that each party involved follows the regulations. Although blockchain technology may offer insight in the entire audit trail, a shared centralized database could achieve the same. This database could be managed by the highest auditing authority in this grape scenario, as this is the final trusted party in the supply chain. Therefore, as there may exists a TTP, according to Wüst and Gervais [**?**], there is no technical rationale to use a blockchain in this scenario.

Philosophical beliefs.

In this scenario, blockchain technology is used as an alternative to a centralized solution. However, in any solution for this supply chain scenario, some form of trust is third parties is unavoidable, because trust has to be placed in auditors that audit the entire certification process. Furthermore, there is also trust in the shipping company for not changing the content of the grape boxes. For example, it would be feasible to exchange the contents of the boxes containing organic grapes with those boxes containing non-organic grapes during transport. Therefore, in essence, trust is placed in the integrity of the information stored on the blockchain. All participants rely that the information on the blockchain is correct only by trusting the auditors.

Network effects.

As blockchain is a complex technology, companies may experiment with it by creating proof of concepts. Indeed, the aim of the original scenario [**?**] was to provide a proof of concept based on blockchain technology. As other technologies, such as a centralized database, seem not to be considered, we assume that the use of blockchain technology is also driven by curiosity.

Economic incentives.

It benefits the technology supplier (here IBM) to use blockchain in this scenario, as it may provide related consulting services. Furthermore, the successful implementation of its technology serves as a platform for future scenarios. In such scenarios both the technology as well as consultancy may be provided. We therefore argue that, although by using blockchain the process of tracking grapes is improved, in this scenario blockchain adoption is also driven by company principles.

Furthermore, in this scenario FOMO may also be a driver for blockchain adoption. Here, FOMO applies to all parties involved considering the potential of blockchain technology. However, as other technologies are not considered in [**?**], only blockchain seems to offer a solution to track certificates.

Breaking the gridlock.

In this scenario several parties (e.g. grape farmers, certification authority, auditors) need to cooperate. None of these parties will come up with a single system that improves the supply chain, as none of these parties is willing to provide a single system that benefits all. Here blockchain technology may have broken down organizational barriers, which triggers collaboration of all parties involved.

Furthermore, as these parties likely do not have the necessary expertise to manage a blockchain, a trusted third party (IBM) managing this technology also triggers company collaboration.

3.4 | Scenario 4 - The BikeBlockchain

Scenario description.

Despite that the number of bikes in the Netherlands is larger than the number of its inhabitants [**?**], bike theft is a common problem. Reporting a bike theft requires the owner of the bike to provide information, such as bike registration number and proof of insurance, to both the local law enforcement and insurance company.

To ease the process of reporting a bike theft, the Dutch Road Transport Authority (RDW) together with IBM have developed the BikeBlockchain [**?**]. This proof-of-concept initiative is based on IBM's Hyperledger Fabric, a permissioned ledger, and is hosted in IBM's cloud solution Bluemix.

Bikes that contain a so-called smart lock can be tracked via the blockchain, as its registers both locking and unlocking the bike, as well its current location. Once a bike is purchased, its new owner can register all relevant information on the BikeBlockchain through a smartphone app. If the bike is stolen, its former owner can simply report this fact through the app. The app will verify if the bike was locked, as unlocked bikes reported stolen are not insured, and send the relevant information to the local law enforcement. After several verification checks a warrant is made and the insurance company is informed. Then the former bike owner is informed if and for how much the insurance can cover the bike theft.

Scenario properties.

Every time a bike is registered, its state (location, locked or unlocked, and bike registration number) is initially written to the blockchain. Bikes are equipped with a smart lock that registers its state (location, locked or unlocked) at frequent intervals to the blockchain. Multiple writers (i.e. locks) are present in this scenario, as anyone can register their bike containing a smart lock. Initial writers must be known, otherwise a malicious actor could register any bike and claim its ownership. Bike owners are not trusted, as the lock reports the its current state. For example, a bike could be stolen when unlocked. However, when manually reporting the theft, a bike owner could report the bike stolen in a locked state. We do not want public verifiability of state, as both the location and ownership of the bike is registered. This would significantly impact the privacy of registered bike owners. Finally, there exists a trusted third party, namely the local law enforcement. Therefore, an alternative solution would be the use of a shared central database. For example, local law enforcement could manage the database, and ensure its integrity. Bike owner could register their bikes in this database, whereas insurance companies could have read access to this database. We conclude that, according to Wust and Gervais [**?**] and Koens and Poll [**?**], there is no need for blockchain in this scenario from a technical perspective.

Philosophical beliefs.
Following the previous conclusion, blockchain technology is used as an alternative system as opposed to other technical solutions, in this case a shared central database. It is interesting to note that there is a commonly known trusted party present, i.e. local law enforcement. In this scenario the role of a the law enforcement as a trusted third party is set aside in favor of blockchain technology. In fact, it is that the technology itself, rather than the actual problem, is leading the solution. This leads to a new driver, namely, technology push, in contrast to problem focus.

Network effects.
Blockchain technology *could* be a solution to ease the process of reporting stolen bikes. But clearly it is not the best technical solution, given its current challenges, such as privacy issues and lack of interoperability with other existing solutions. However, the hype around blockchain may have triggered the use of blockchain in this scenario.

Economic incentives.
IBM is the owner of Bluemix, a cloud service. Furthermore, blockchain solutions provided by IBM are based on Hyperledger Fabric. There is a strong economic incentive for IBM to use their solution, as it both generates media attention thus marketing their product, as well as creating revenue.

Furthermore, the current process of dealing with stolen bikes is cumbersome for all parties involved. Using blockchain improves this process as parties are more aligned, and dealing with a reported stolen bike becomes much more easy for all parties involved.

Breaking the gridlock.
There is an economic incentive for the parties involved to improve the process of stolen bikes registration. For example, reducing paper work when dealing with stolen bike registration at both the insurance company and law enforcement would decrease administrative overhead. However, up until now no party has taken up the initiative. Here blockchain also breaks down organizational barriers, as this technology creates a means and possibility to collaborate between insurance companies, law enforcement, and RDW.

Also in this scenario it is unlikely that these parties currently have the knowledge to manage a blockchain. IBM as a third party managing Hyperledger Fabric also triggers organisational collaboration.

3.5 | Scenario 5 - MedRec

Scenario description.
In this scenario blockchain is used as an interoperability solution between multiple medical databases stored at different providers of medical care. A type of Ethereum blockchain is used in a private peer-to-peer network. The data stored in the blocks represents data ownership and viewership permissions, no actual patient data is stored on the blockchain. However patient meta-data in the form of patient-provider relationships are logged [**?**], with viewing permissions and data retrieval instructions (these are pointers) for execution on external databases. Also a hash of the record of the underlying medical database is stored, with the aim to guarantee integrity of the patient record data.

Providers can add a new record for a patient. Patients then can authorize the sharing of records between providers. In both cases, either the provider or the patient receiving new information receives a notification and can verify the proposed change before accepting or rejecting the record.

Identities are managed through a DNS-like server, where Ethereum addresses are linked to real world names or social security number.

Miners use their computational resources (PoW) to solve a puzzle and be able to determine the next state of the blockchain. Ekblaw et al. [**?**] envision that medical researchers and health care stake holders mine in the network. In return, providers and patients allow limited access to aggregated, anonymised data as a mining reward. Thus, the incentive for a miner is to be able to obtain data, for example, the average iron levels in blood samples across all patients in the previous week [**?**]. Ekblaw et al. [**?**] foresee that in future work miners can request specific (anonymised) data in return for their efforts.

Ekblaw et al. [**?**] consider the following properties to be benefits of this system:

- Robustness. Due to the peer-to-peer network there exists strong resilience, and there is no single point of failure.
- Security. The blockchain is not a central point of attack to obtain medical data, compared to a centralized approach.
- Privacy. No medical data is stored on the blockchain (although patient meta-data is stored on the blockchain).
- Interoperability. MedRec facilitates continuous use of existing systems.

Scenario properties.

Although the MedRec blockchain may be, to some extent, decentralized, Ekblaw et al. [**?**] do not go into much detail on identity management and the off-chain syncing algorithm between the blockchain and the medical databases. For example, as MedRec is a private blockchain, someone has to provide access to the ledger. This is in contrast to public Ethereum, where there exists no central doorman. Thus in this scenario a central party exists, defeating the purpose of a blockchain.

Second, MedRec uses PoW in a private setting. Besides that other consensus algorithms are more suitable for such a setting, like BFT, it allows attacks on the network. For example, the well-known 51% attack would allow a single miner to obtain all rewards, and with that exclude other miners from rewards. Additionally, there is an incentive for nodes to delay PoW solutions. For example, in a private peer-to-peer setting a node may delay the solution to the PoW puzzle, as this would increase the probability of finding the solution to the PoW puzzle by the delaying node. If we assume that all participants are honest, and each participant mines with the same amount of computational power, then the distribution of rewards would be equal amongst all participants. Again, instead of using PoW, a BFT type consensus algorithm does not require a large amount of computational resources and additionally participants may be regarded for each BFT vote they provide. This would provide the same incentive and equal distribution of rewards amongst the MedRec miners.

The benefits of using a blockchain for MedRec can also be achieved by other technologies [**?**] [**?**]. In fact, blockchain is useful for achieving consensus amongst a consortium of unknown participants [**?**]. Indeed, in this use case writers are known, there is no need for public verifiability, and given the sensitivity of medical data using a trusted third party may be a better solution than depending on a set of untrusted parties aiming to reach consensus. Therefore, the need for blockchain is not justified in the MedRec use case.

Philosophical beliefs.

MedRec aims to facilitate so-called precision medicine, a model that aims to facilitate customization of healthcare being tailored to that of the individual patient, without the creation of a central repository of data. Indeed, MedRec claims that because the medical data stays decentralized, the system does not create a single target for content attack. However, the system provides a database with pointers to records of medical data. In essence, MedRec does provide a single point of attack which accurately shows which provider stores which medical data. This in itself can be leveraged for targeted attacks, for example, to exactly determine where patient data is stored at which provider.

Network effects.

The MedRec paper explores how blockchain can be used within a medical environment. However, it fails to address any other type of technologies that may also be suitable for this particular problem. Given the current hype on blockchain technology, we assume that MedRec is also inspired by the current blockchain hype.

Economic incentives.

The work on MedRec [**?**] [**?**] does not show economic incentives that drives blockchain adoption, by any of the participants.

Breaking the gridlock.

In this use case blockchain also is not the best solution from a technical perspective. However, there is an incentive to cooperate between the parties a it eases the process of sharing patient data between medical institutes, with the consent of the patient. Therefore, Ekblaw et al. [**?**] may have chosen blockchain as it can trigger collaboration between the various medical institutes.

The use case does not address which party, eventually, will manage MedRec (e.g. software updates). Similar to the supply chain and identity management use case, it is likely that a single party will manage MedRec. This is also a driver for organisations to collaborate, as they do not need specific technological knowledge to use MedRec.

3.6 | Scenario 6 - Smart Grid

Scenario description.

Jouliette is a project using a blockchain-based solution to, primarily, record energy production and consumption, and enable trade of energy and other items of value based on this. To fully appreciate blockchain adoption drivers for Jouliette, it is important to note that the idea of Jouliette came into being around the same time as Nakamoto's Bitcoin was created: in 2009, during the financial crisis [**?**]. Envisioned by Jos Blom at Alliander (a Dutch electricity network operator), essentially the idea was to create a new gold standard based on energy production: producing some amount of sustainable energy would provide some kind of credit, which could later be traded back for sustainable energy. At this point, blockchain was not yet widely known or available: this idea did not come into being as "a blockchain idea".

Around 2016, Spectral Energy became interested in piloting this project. Based at the community of De Ceuvel, Spectral is a technology company specializing in clean technologies. De Ceuvel is a small community of boats, that are rented out to parties for commercial purposes (art studios, cafés, etc), but not for residence. Their focus is on community participation and sustainability. Most boats are equipped with solar panels, and there is a local private microgrid that could in principle run disconnected from the regional energy grid (managed by the grid operator) [**?**]. They have a single connection to the regional energy grid, and a single contract with an energy supplier for the entire community. They are free to manage the microgrid in the way they choose, and therefore they were a very suitable location for piloting this project. We note that there have emerged some differences between Blom's *vision* of Jouliette, and the *implementation* of the pilot project. We will attempt to keep this distinction clear.

Blockchain technology was first identified as a potential basis for Jouliette in 2015 [**?**]. The Jouliette token itself is best described as a blockchain-based asset-backed token that uses a unique method of mining. Rather than a Proof of Work-based algorithm, a Jouliette is created when a certain amount of electricity from renewable energy sources such as solar panels is generated. Jouliette can be traded amongst users. A secondary token, Ceuveltje, exists at De Ceuvel. This is a speculative token mined "for free" by the café, as a sort of loyalty token that is tradeable for

Jouliettes[2] [**?**].

Follow-up projects are being explored with Schoonschip, a similar community as De Ceuvel; and the municipality of Groningen, where the technology will be applied to common grid infrastructure using smart meters and Spectral's hardware [**? ?**].

Scenario properties.

Because the Jouliette as envisioned did not include the speculative token Ceuveltje, we will focus on the technical aspects of the main Jouliette token and its implementation. We do note that we believe Ceuveltje could be replaced by any other form of value transfer, be it bitcoin, money, or eggs.

The Jouliette needs to store state: because it is intended to implement a non-speculative token, it needs to store what amount of energy was produced or consumed when and where [**?**]. However, state does not have to be publicly verifiable. Every participant that *needs* to be able to verify the state is also a writer.

In interviews performed by Bekhuis [**?**] and in personal communication with Alliander, the view that energy systems should be open and accessible to everyone is emphasized. This flows from Alliander's role of a network operator: if they create infrastructure solutions, everyone needs to (be able to) use them. So anyone should be able to join the system. Thus, there are multiple writers: essentially, every (micro)grid connection needs a writer. From the perspective of a participant, not all these writers are known. At De Ceuvel, a small community, it may be the case that all writers know each other, but that is emergent from the location of the pilot, not a technical aspect of the Jouliette as envisioned. Since it should be possible to freely trade Jouliette, a participant needs to be able to verify that any other participant is playing by the rules. This presents a problem: the essence of the Jouliette token is that it is *directly* backed by energy that has actually been produced at a certain moment. But in contrast with a hard computational problem as in Bitcoin, this is not something that participants can verify. This is similar to the supply chain scenario, except now we're recording energy instead of grapes. So we need trusted hardware to measure a participant's real energy production or consumption and to turn that into Jouliettes on the blockchain. In the case of De Ceuvel, hardware performing both tasks was purpose-built by Spectral. In follow-up projects, such as in Groningen, the measurements may be provided by a smart meter, but they still need additional hardware to interact with the blockchain[3]. By Spectral's own documentation, this hardware is tamper-proof [**?**]. This implies they do not trust the participants for whom the hardware is writing. The fact that the hardware needs to be tamper-proof shows the source of trust of the scenario: the hardware implements a *trusted writer*.

This leaves us with a conundrum: How can we have a case where hardware is implementing trusted writers, but those writers are not all necessarily known to participants? We seem to have a mix between the Supply Chain scenario, where some record of physical objects is put on a blockchain making heavy use of certification authorities and auditing authorities; and the BikeBlockChain scenario, where the lock is trusted but does need to be known initially. The trusted hardware here is effectively such a lock, and *must* be verified as trustworthy when first added to the system. In the implementation at De Ceuvel, Spectral, as the supplier of both soft- and hardware that implements the trusted writers, is effectively a Trusted Third Party. But the scenario should allow for hardware created by other parties.

Who could take on the role of this TTP in this scenario is unclear. At face value, the electricity network operator

[2] The reason for the existence of this secondary token is not immediately evident: why not just make it possible to trade Jouliettes for money directly? However, that would put the Jouliette in the realm of cryptocurrency and money, and make it susceptible to speculation and regulation. It would also mean that Alliander might not be allowed to continue the project, because strict regulation exists about what a network operator can and cannot do [**?**].

[3] Tamper-evident smart meters provided by the grid operators, as used in the Netherlands, could provide the required data to directly connected third-party hardware, but hardware consuming the data from the smart meter cannot currently verify that the data is actually coming from the smart meter itself [**?**]. So this connection and the hardware consuming the data should itself be tamper-proof or tamper-evident in order to be trustworthy.

could function as a TTP: they provide a public service that everyone needs to trust them to deliver anyway. However, regulations exist that limit the allowed activities of a network operator, to prevent that e.g. individual energy suppliers are unfairly (dis)advantaged by the network operator. Whether a network operator would be allowed to take on the role of TTP under these regulations is unclear to us. But the need for this TTP exists, so some solution must be found. Because this TTP only needs to verify hardware when added, however, it is *not* necessarily an *always-online* TTP and therefore its necessity doesn't result in a rejection of blockchain technology based on the presence of a TTP[4].

If we now follow the scheme from Wüst and Gervais [**?**], we find that we can answer both the questions "are all writers known?" and "are all writers trusted" with yes: tamper-proof hardware implements a trusted writer, even though the participant it represents may not be trustworthy. This leads to the conclusion that a blockchain should not be used. If instead we follow Koens and Poll [**?**], we get a more nuanced answer: participants are known, and not everyone can join the network[5], so we end up with a distributed ledger. When blockchain was first introduced in this project, in 2015, the technology landscape looked different and there may not have been a viable option for a distributed ledger, as opposed to Multichain. However, Spectral has changed its implementation once already from Multichain to Sawtooth [**?**], and Blom has stated that the current technology still has shortcomings [**?**], so it is entirely possible that Jouliette will move towards a different technology again in the future.

In personal communication, the availability aspect of *distribution* (as opposed to decentralization) was deemed important; we merely note that distribution is possible without a blockchain.

Philosophical beliefs.

Interviews performed by Bekhuis show that the Jouliette as envisioned has a large philosophical component [**?**]. When it was first envisioned, during the 2009 financial crisis, the main idea was to make it possible to use sustainable energy directly as the basis for a barter system. This would effectively create a new "gold standard" for energy trading, because it would be backed by actual energy production and consumption. The main drivers for this were to prevent the speculation as seen in the fiat money system, and to stimulate sustainable energy adoption [**? ?**]. Thus, Jouliette is intended to keep a record of the *physical* aspect of energy flows, not the financial aspect. There is no requirement to back Jouliettes with monetary value, to ensure that the technology is flexible enough so that users can determine their own rules. If they choose to sell tokens for money, they would be free to do so; or if they choose to only trade Jouliettes for energy (e.g. exchange their surplus by day for free consumption by night), this is possible, too [**?**].

Regulation in the Netherlands is such that individual consumers are not allowed to trade their energy surplus. Instead, the energy surplus is effectively sold back to their energy supplier under a netting scheme: the energy provided back to the electricity grid is subtracted in its entirety from the energy consumed from the electricity grid. If a consumer produces more energy than they consume, they are still obligated to sell it back to their energy supplier; but in that case the energy supplier can simply offer a much lower price for the energy. The creator of Jouliette believes this system is needlessly restrictive, and this regulation should be changed [**?**], so that individual consumers can trade with other individual consumers. He also believes that this would lead to consumers potentially simply giving away energy rather than trading it, without (immediate) compensation. However, in the pilot project, it seems that users prefer monetary compensation over social benefits. To encourage the users to start trading peer-to-peer, a second

[4] At De Ceuvel, initially the open-source platform Multichain was used. Spectral switched to the Hyperledger Sawtooth platform [**?**].

Sawtooth uses a consensus algorithm that uses trusted hardware in the form of Intel's SGX platform. Though it may look like this eliminates the need for a TTP, or puts Intel in the role of this TTP, notice that SGX only verifies that the correct *code* is running on an SGX platform. This is required for the correct functioning of Sawtooth, but it does *not* verify that the code is provided with measurements from trustworthy sources, so we still need a TTP to certify the entire hardware platform.

[5] This does not mean that participants are kept out; instead, it reflects the *requirement* to have certified trusted hardware to join the network. Of course everyone should be provided with such trusted hardware.

speculative token has been introduced at De Ceuvel alongside the Jouliette, called Ceuveltje. This token is intended to take the role of speculative cryptocurrency that can be traded for Jouliette, and can be used locally in e.g. the café for discounts. Whether this incentivizes users enough to start trading peer-to-peer is still an open question [**?**], but it is clear that for different parties, different incentives seem to exist. Interestingly, Spectral explicitly argues against this model of a secondary token in [**?**], but there is clearly a difference between the vision and the implementation.

So we see a clear belief in an alternative system, and a political stance about how the system should be (de)regulated.

Alliander has stated that it thinks a decentralized model with greater local interaction is needed for the energy transition, and that it hopes that projects like the Jouliette enable this [**?**]. However, we note that decentralization can also be achieved without a blockchain.

Network effects.

Curiosity of whether blockchain was fit for this scenario may seem to have been a driver. However, the project was not exploratory: the team was convinced that blockchain technology was fit for purpose based on technical merits and philosophical beliefs [**?** , personal communication]. We conclude network effects have played little to no role.

Economic incentives.

There seem to be no direct economic incentives in play for blockchain adoption for Jouliette as envisioned by Alliander, nor for De Ceuvel in the pilot project. The only economic aspect we have found is a process improvement mentioned by Spectral: energy suppliers sometimes bill incorrectly due to basing the consumption on estimates, rather than real measurements [**?**]. Using a blockchain as a record for energy consumption and production should eliminate this entirely, which leads to cost savings for the customer. However, smart meters are read monthly by the grid operator, the blockchain solution uses the same data from the smart meters, and it is not made clear what the added advantage of a blockchain is over using the data from the grid operator. We are under the impression that this is a post-hoc "added benefit" which happens to emerge from using blockchain, rather than that it played a role as a real adoption driver.

Breaking the gridlock.

Blockchain technology itself did not seem to play a significant role in triggering collaboration between Alliander and Spectral. However, Alliander's vision of the Jouliette clearly does have some elements of inducing organisations to collaborate towards a better energy system [**?**].

4 | DISCUSSION

For our discussion we assume that the scheme of Wüst and Gervais [**?**] is correct, and we assume that our list of drivers is complete. This means that all technical conditions in their scheme must be met to ensure the appropriateness of using blockchain. However, in the uPort, supply chain, BikeBlockchain, MedRec, and smart grid scenarios only some conditions are met. Blockchain is used in all of these scenarios despite that there appears to be no technical rationale to use blockchain, according to the scheme of Wüst and Gervais [**?**]. Clearly, the technical conditions in [**?**] alone are insufficient in explaining blockchain adoption.

Given the assumptions in the previous paragraph, we observe from Table 1 that the majority of drivers for blockchain adoption in each of the six scenarios is non-technical. However, the technology supports at least one underlying technical property in a scenario, such as storing of state. Therefore, we conjecture that blockchain adop-

tion is driven by a combination of both technical and non-technical drivers.

Furthermore, we observe that in each scenario a TTP *could* be used. Therefore, blockchain technology is not needed for any of these scenarios, according to [**?**]. However, in the Bitcoin scenario there used to be an underlying academic problem, namely, how can a consortium of unknown and unbounded number of participants reach consensus. Nakamoto [**?**] aims to answer that question by introducing blockchain technology. Therefore, a rationale exists to use blockchain in the Bitcoin scenario.

5 | RELATED WORK

Although several models exists to determine technology acceptance, the Technology Acceptance Model [**?**] is most employed [**?**]. Blockchain technology and the Technology Acceptance Model (TAM) are discussed in, for example, [**?**]. TAM is used to determine technology adoption based on two major considerations, *perceived usefulness* and *perceived ease of use* by the intended user. Depending on the research domain, TAM has been extended with other considerations such as 'perceived playfulness' for the web acceptance, and 'perceived user resources' in bulletin boards systems [**?**]. In our work we distinguish four considerations (i.e. the driver categories) for the adoption of blockchain.

Baur et al. [**?**] use TAM to identify adoption drivers and barriers of cryptocurrencies, in particular Bitcoin. Cryptocurrencies are a particular application of blockchain technology. Therefore, the drivers identified in the work of Baur et al. do not necessarily relate to blockchain.

Debabrata and Albert argue that blockchain may eliminate fraud in supply chain management [**?**]. However, eliminating fraud only by using a blockchain in the grape scenario is impossible. A TTP must remain present to verify the claims made by the farmers, certification authorities, and accreditation authorities. Here, blockchain cannot replace the trust in human observation of a complex process.

Wang et al. [**?**] propose a maturity model for blockchain adoption. In their work the five stages of maturity from the ACM Computing Classification System is used to determine the maturity of blockchain. From this description, Wang et al. conclude that blockchain currently is not ready for adoption, as there are multiple technical issues such as scalability. However, the current limitations of blockchain may not always be an issue. For example, blockchain could be applied in a use case where scalability is of no importance. Therefore, we argue that creating a maturity model for blockchain adoption is only useful given a particular use case. In our work we described six use cases, and discussed the rationality of blockchain adoption. We have shown that blockchain adoption goes beyond technological choices, as it is clear that in most use case the non-technical drivers drive blockchain adoption.

Batubara et al. [**?**] state that there are several barriers for blockchain adoption. Hence, they provide a systematic overview of the challenges of blockchain adoption for e-government, and group these challenges into three aspects: technological, organisational, and environmental. Despite these barriers and challenges, we observe that blockchain is adopted in various industries, including government. In our work we analyse the drivers behind this adoption.

In contrast to our work, [**?**] Hackius and Petersen discuss barriers for blockchain adoption, in particular in the logistics sector. They provide seven potential barriers that may lead to *not* adopting blockchain. Interestingly, the barrier 'Dependence on Blockchain operators'is in our work considered a blockchain adoption driver, namely 'Third party transfer'. This difference may be explained by the weight of the drivers. Some drivers may have a stronger influence on blockchain adoption than other drivers. Determining the weight for each driver is a subject for future work.

Seebacher and Schüritz propose that the qualitative aspects of transparency and autonomy play a role in blockchain adoption [**?**]. In addition to these two aspects, in our work we argue that blockchain adoption lies in both the technical

and non-technical drivers, and we identified a total of 24 drivers.

Finally, in this extended version of [**?**], we include three additional scenarios, one new driver category and three new non-technical drivers.

6 | FUTURE WORK

In our work we have shown that technical and non-technical drivers exist for blockchain technology adoption. Various models have been suggested to support this decision making process, as discussed in Section 2. These models, however, do not mention alternatives to blockchain. A further analysis, and a possible extension of these models is needed to determine if blockchain is appropriate.

Also, trust in a third party appears to be a much broader concept than the trust a blockchain can offer. In fact, this technology appears to provide trust in integrity of the data recorded on the blockchain. However, we assume that the trust needed by a participant goes beyond integrity of data alone. Therefore, it is unlikely that blockchain can fully replace a TTP. Additionally, the concept of trust has been defined in many ways [**?**]. For example, one way of defining trust is the willingness to depend, meaning that you make yourself vulnerable to another person in a situation by relying on them [**?**]. However, these many definitions also makes that the concept of trust is diffuse, and it is unclear what is defined as a *Trusted* Third Party. How blockchain shifts trust, and which types of trust are affected by blockchain also seem interesting subjects for further exploration.

As we made the assumption in Section 4 that our list of drivers is complete, additional scenarios can be analysed to determine if more non-technical drivers exists. Also, we assumed in Section 4 that the scheme by Wüst and Gervais [**?**] is correct. A further analyses of this scheme can be performed to determine if additional technical drivers exist. Our research can also be extended by analysing the responses of the authors of the scenarios addressed in our research, regarding the assumptions made on the use of blockchain in their scenarios. All three analyses will further improve the validity of our results.

Furthermore, extending our research by adding weights to the drivers may be part of future work. Adding weight to drivers allows for determining which driver influences blockchain technology adoption the most.

Interpretative variations may exist for, in particular, the non-technical drivers. We believe additional research can tell whether the drivers impact on the beliefs of individuals in an organisation. Finally, to gain insight in the potential variations of non-technical drivers, refinement of these categories (for example, philosophical beliefs and breaking the gridlock) is needed. This allows, for example, for determining if there exists a consensus on the drivers across organisations and sectors.

7 | CONCLUSION

Many people have questioned the rationale behind blockchain adoption [**? ?**]. To support such claims, methodologies have been proposed to see if blockchain suits a particular scenario [**? ?**]. Such methodologies are mainly based on technical drivers, which are properties inherent to a scenario. In real-life scenarios we see that sometimes a blockchain-based solution is chosen even if these methodologies would argue against that.

Given the inherent lack of technical drivers in some scenarios, the choice for blockchain technology may seem irrational. Our novel insight is that blockchain adoption may be explained by non-technical drivers, namely philosophical beliefs, network effects, economic incentives, and breaking the gridlock. These drivers may explain, after all, the rationale behind blockchain adoption. Our work can be generalized to other scenarios that involve cryptocurrencies,

identity management solutions, and supply chains, as it is likely that similar scenarios contain the same drivers.

TABLE 1 Summary of use case analyses: Blockchain technology adoption drivers

Category	Drivers	*Bitcoin*	*uPort*	*Supply Chain*	*BikeBlockchain*	*MedRec*	*Smart Grid*
Scenario properties	Storing state	•	•	•	•	•	•
	Multiple writers	•	•	•	•	•	•
	Can not use TTP	•					
	Writers unknown	•	•				
	Writers untrusted	•				•	
	Public verifiability	•	•	•			
Philosophical beliefs	Will not use TTP	•					
	Decentralization need	•	•			•	•
	Enhanced privacy	•	•				
	Alternative system	•	•	•	•	•	•
	Political reasons	•					•
	Technology push				•	•	
Network effects	Driven by community	•					
	Curiosity	•	•	•		•	
	Cool to use	•	•	•		•	
Economic incentives	Marketing product		•	•	•		
	Selling mining equipm.	•					
	Selling consultancy	•		•	•		
	Charging for platform			•	•		
	FOMO	•		•			
	Alternative investment	•					
	Process improvement			•	•		•
Breaking the gridlock	Organisational push		•	•	•	•	•
	Third party transfer		•	•	•	•	